

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-66592

(P2000-66592A)

(43) 公開日 平成12年3月3日(2000.3.3)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 B 5 J 0 4 9
G 0 6 F 7/58		G 0 6 F 7/58	A
H 0 3 K 3/84		H 0 3 K 3/84	Z

審査請求 未請求 請求項の数 5 O L (全 5 頁)

(21) 出願番号 特願平10-232823

(22) 出願日 平成10年8月19日(1998.8.19)

(71) 出願人 596131492

システム工学株式会社

東京都千代田区神田錦町1-15-11

(71) 出願人 396020800

科学技術振興事業団

埼玉県川口市本町4丁目1番8号

(72) 発明者 長井 剛一郎

神奈川県相模原市御園3丁目2番7号

(74) 代理人 100079119

弁理士 藤村 元彦

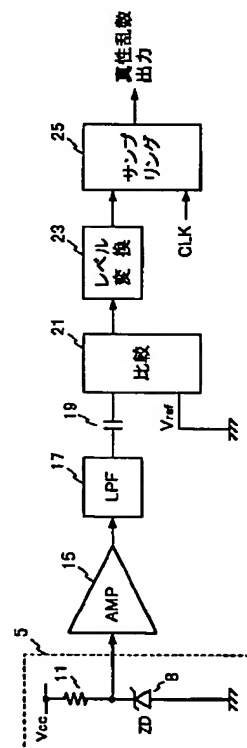
Fターム(参考) 5J049 AA00 AA14 AA15 BB01 CB01

(54) 【発明の名称】 乱数生成装置

(57) 【要約】

【目的】 暗号理論的に安全な2値乱数を容易に生成することが可能で、小型化に適した乱数生成装置を提供する。

【解決手段】 接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を接合に印加する逆バイアス印加手段と、接合を含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、を有する。



【特許請求の範囲】

【請求項1】 接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を前記接合に印加する逆バイアス印加手段と、前記接合を含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、からなることを特徴とする乱数生成装置。

【請求項2】 前記雑音信号の増幅信号を得る増幅回路と、

前記増幅信号を所定の基準電圧と比較して2値化信号を得る比較回路と、

前記2値化信号をサンプリングして、0及び1からなるサンプリング値系列を得るサンプリング回路と、を有することを特徴とする請求項1記載の乱数生成装置。

【請求項3】 前記半導体素子は、ツェナーダイオードであることを特徴とする請求項1又は2記載の乱数生成装置。

【請求項4】 前記サンプリング値系列における0及び1の各々の発生確率が略等しくなるように前記基準電圧を制御する制御手段を有することを特徴とする請求項2又は3記載の乱数生成装置。

【請求項5】 前記サンプリング値系列における0及び1の発生確率が略等しくなるように前記サンプリング値系列を平滑化する手段を有することを特徴とする請求項2又は3記載の乱数生成装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は乱数生成装置、特に、暗号化アルゴリズムに用いられる乱数生成装置に関する。

【0002】

【従来の技術】インターネット、イントラネットの発展に伴い国際間取引、異業種取引、電子データ交換（EDI：Electronic Data Interchange）などの新市場の開拓が盛んに行われている。一方、インターネットのオープン性から、ネットワーク上を往来する情報に対する不正行為（盗聴、改ざん、なりすまし、破壊行為等）への対応が必要であり、セキュリティ技術の開発が急がれている。

【0003】ネットワークのセキュリティを確保するために広く暗号が利用されており、例えば、米国で標準化されているデジタル署名アルゴリズム（DSA）がある。このような暗号化アルゴリズムにおいては、署名生成の度に乱数を生成させる必要があるが、用いる乱数としては「情報（暗号）理論的に安全な乱数」であることが望ましい。

【0004】暗号理論的に安全な乱数とは、「乱数列の任意の一部から他のビットを多項式時間で推測できない」という条件を満たす乱数をいう。しかし、この条件はかなり厳しいので、実用上は以下のような評価尺度が

用いられることがある。但し、これらはあくまでも必要条件に過ぎない。

（1） 0, 1の等頻度性

（2） 長周期性

（3） 非線型性

（4） 線形複雑度が大きいこと

（5） 無相関性

非線型性というのは、乱数が線形フィードバックシフトレジスタ（linear feedback shift register）の出力そのものではないということである。n段の線形フィードバックシフトレジスタで生成できる系列の最大周期は $2^n - 1$ であり、この周期 $2^n - 1$ の系列をM系列（maximum length shift register sequence）と呼ぶ。従って、擬似乱数としてよく用いられるM系列はこの基準を満たしていない。

【0005】乱数系列の線形複雑度とは、その系列を生成する最小等価な線形フィードバックシフトレジスタの段数を指す。上述の周期 $2^n - 1$ のM系列を例にとると、これはn段の線形フィードバックシフトレジスタで生成される最大周期の系列であるので、M系列の線形複雑度はnである。線形複雑度が小さいと、容易に等価な乱数発生器が構成できるので、未知ビットの推測が容易で、暗号学的に安全な乱数とは言えない。

【0006】無相関性は、例えば、乱数のビットが他の部分と独立であることを意味し、逆に相関性があると未知のビットの推測が容易となることを意味する。従来、暗号化アルゴリズムの乱数源として擬似乱数が一般に用いられてきた。しかしながら、上記した観点から擬似乱数は暗号学的に安全な乱数とは言えない。すなわち、擬似乱数は一定の算術プロセスあるいは関数の組合せから生成されるため、同じ初期条件を与えることにより同一の乱数を発生させることが可能である。従って、擬似乱数を用いた暗号は、生成法の推測も可能であり、破られやすく、秘密性の保持の点において不十分であった。

【0007】一方、全くランダムな真性乱数に近い乱数を発生させる方法としては、自然現象、例えば放射性物質の崩壊現象等を利用した装置などがあるが、装置が大きく複雑であるという欠点を有している。従って、秘密性が高く、パーソナルコンピュータ等に容易に組み込み可能な小型の乱数生成装置の実現が要望されている。

【0008】

【発明が解決しようとする課題】本発明はかかる点に鑑みてなされたものであり、その目的とするところは、暗号理論的に安全な2値乱数を容易に生成することが可能で、小型化に適した乱数生成装置を提供することにある。

【0009】

【課題を解決するための手段】本発明による装置は、接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を接合に印加する逆バイアス印加手段と、接合を

含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、を有する。

【0010】

【発明の実施の形態】以下に本発明の実施例を図面を参照しつつ詳細に説明する。図1は、本発明による第1の実施例である乱数生成装置の構成を概略的に示している。また、図2は図1に示した乱数生成装置の動作を説明する図であり、主要な回路ブロックの出力信号を示している。

【0011】図1において、5は雑音発生回路である。ツェナーダイオード8のp n接合に抵抗器11を介して降伏が生じる程度の逆バイアス電圧を印加している。これにより、逆方向に微弱な降伏電流が流れ、ランダムな雑音電圧が発生する。このようにツェナーダイオード8を動作させることにより、ツェナ電圧を中心とした、ピークトゥーピーク（peak-to-peak）で数十〜数百 μ V程度のランダムな雑音電圧出力が得られ、これを乱数の発生源としている。

【0012】具体的には、電源電圧 V_{cc} を+12Vとし、ツェナーダイオード8にはツェナ電圧が6.3Vと電源電圧の約1/2であるものを用いた。ツェナーダイオード8には560k Ω の抵抗器11を介して逆バイアス電圧を印加することにより、約10 μ Aの逆方向電流が流れ、6.3Vを中心にpeak-to-peak電圧が約20 μ V、平均周波数が60〜70kHz程度の雑音電圧が発生する。（図2（a）参照）

雑音発生回路5で得られた雑音電圧は微弱であるので、これを増幅回路15を用いて電圧増幅する。具体的には、2段のオペアンプを用いている。この増幅回路15の電圧利得は約74dBで、6.3Vを中心としたpeak-to-peak電圧が1V程度の増幅出力を得ることができる。（図2（b）参照）

次に、増幅回路15により増幅された雑音出力は、ローパスフィルタ17に供給され高周波成分が除去される。ローパスフィルタ17のカットオフ周波数は、後述するサンプリングの周波数の数倍程度以上であればよい。ローパスフィルタ17の出力は、比較回路21に供給され、所定の基準電圧を閾値としてハイレベル、ローレベルに分けられ2値化される。

【0013】増幅雑音出力は、ツェナ電圧6.3Vを中心にはほぼ対称であるので、ツェナ電圧を基準電圧として増幅雑音電圧の2値化を行うことができる。本実施例においては、基準電圧として非常に安定している接地電圧を用いている。すなわち、結合コンデンサ19を用い、増幅雑音出力の直流成分をカットした交流成分を比較回路21に入力している（図2（c）参照）。これにより、接地電圧（0V）を閾値とした2値化を行うことができる。この構成においては、温度変化によってツェナ電圧が変化しても、直流成分が増減するのみで2値化に

は全く影響は生じない。従って、比較回路21の入力端には0Vを中心にしたpeak-to-peak電圧が1V程度の増幅雑音電圧の交流成分が入力され、接地電圧である0Vを閾値とした2値化が行われる。

【0014】比較回路21の出力は、レベル変換回路23に入力され、後段のサンプリング回路25の論理電圧レベルに変換される。レベル変換回路23の出力は、周期性のないランダムな矩形波である（図2（d）参照）。この矩形波は、サンプリング回路25に供給される。サンプリング回路25は、入力矩形波の周波数に対してある程度低い（数分の1程度以下の）一定周波数で入力矩形波のサンプリングを行い、0及び1のビットからなる系列を得る。入力矩形波には周期性がなく、またサンプリングのタイミングは入力矩形波の周波数とは独立であるので、得られたビット系列は、0、1の各々の発生確率が等しければ、真正乱数系列であることが期待できる。

【0015】サンプリング回路25において得られた0、1からなる真正乱数の系列は、外部インタフェース（図示していない）、例えばRS-232Cインタフェースなどを介して外部機器へ供給される。尚、サンプリング周波数は、外部機器が必要とするビットレートに設定する必要がある。上記したように、本発明によれば、半導体接合に降伏電圧程度の逆バイアス電圧を印加したとき生じる雑音を乱数の発生源とすることにより、2値の真性乱数を容易に生成することが可能である。また、上記した回路は容易にIC化が可能であり、極めて小型の乱数生成装置を実現することができる。

【0016】従って、本装置を、例えばパーソナルコンピュータ等に「真性乱数発生エンジン」として組み込むことにより、デジタル署名アルゴリズムを用いた署名生成のための「真性乱数（物理乱数）」を提供することができる。すなわち、従来用いられてきた疑似乱数を用いた場合に比べはるかにセキュリティ確度の高い通信を行うことが可能となる。

【0017】図3は、本発明による第2の実施例である乱数生成装置の構成を示している。本実施例が第1の実施例と異なる点は、得られた乱数系列の0及び1の各々の発生確率が等しくなるように制御する制御部31を設けていることにある。すなわち、制御部31は、サンプリング回路25の出力を得て、この出力のうちハイレベル電圧、ローレベル電圧の各々の持続時間の累積値が互いに等しくなるように比較回路21に与える基準電圧 V_{ref} を制御している。

【0018】従って、制御部31を設けて基準電圧 V_{ref} を制御することにより、最終的に得られる乱数系列の0及び1の発生確率を等しくすることができ、より真性乱数に近い2値乱数系列を得ることができる。図4は、本発明による第3の実施例である乱数生成装置の構成を示している。本実施例が第1及び第2の実施例と異なる

点は、サンプリング回路25において得られた乱数系列の0及び1の各々の発生確率が等しくなるように平滑化処理をなす平滑部35をサンプリング回路25の後段に設けていることにある。

【0019】平滑化は、インバランスな0、1の系列を、 x_1, x_2, x_3, \dots としたとき、

【0020】

【数1】

$$y = x_1 \oplus x_2 \oplus \dots \oplus x_n$$

【0021】を用いて行うことができる。ここで、

【0022】

【外1】



【0023】は2を法とする和（排他的論理和）を表す演算である。これにより得られるyの系列はバランス性が改善されることが示される。すなわち、 x_1, x_2, x_3, \dots の系列中の0の発生確率をp、1の発生確率を $q = 1 - p$ とし、yに関して0の出現確率をP、1の出現確率を $Q = 1 - P$ とすると、yのインバランスは、 $P - Q = (p - q)^n$

で与えられる。ここで、nは平滑化におけるブロックサイズである。nを大きくとれば、インバランス性は指数関数的に小さくなる。

【0024】尚、図4においては平滑部35をハードウェアの構成として説明したが、実際はコンピュータのソフトウェアで容易に実現可能であり、コンピュータ側で必要な程度（ブロックの大きさ）で行えば十分である。

以上の処理を行うことによって、より真正乱数に近い

0、1の系列を得ることができる。尚、上記実施例にお*30

*いては、雑音発生源としてツェナーダイオードを用いた場合を例に説明したが、これに限らず、例えば異種導電型の半導体接合を用い、その降伏電流を雑音発生源として用いてもよい。

【0025】

【発明の効果】以上詳細に説明したように、本発明によれば、半導体接合の降伏電流を雑音発生源として用いることにより、暗号理論的に安全な2値乱数を容易に生成することが可能で、かつ小型化に適した乱数生成装置を実現することができる。

【図面の簡単な説明】

【図1】本発明による第1の実施例である乱数生成装置の構成を示す図である。

【図2】図1に示した乱数生成装置の動作を説明する図である。

【図3】本発明による第2の実施例である乱数生成装置の構成を示す図である。

【図4】本発明による第3の実施例である乱数生成装置の構成を示す図である。

【主要部分の符号の説明】

5 雑音発生回路

8 ツェナーダイオード

11 抵抗器

15 増幅回路

17 ローパスフィルタ

21 比較回路

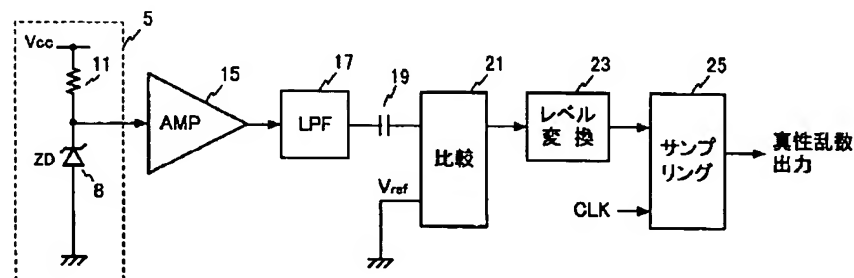
23 レベル変換回路

25 サンプリング回路

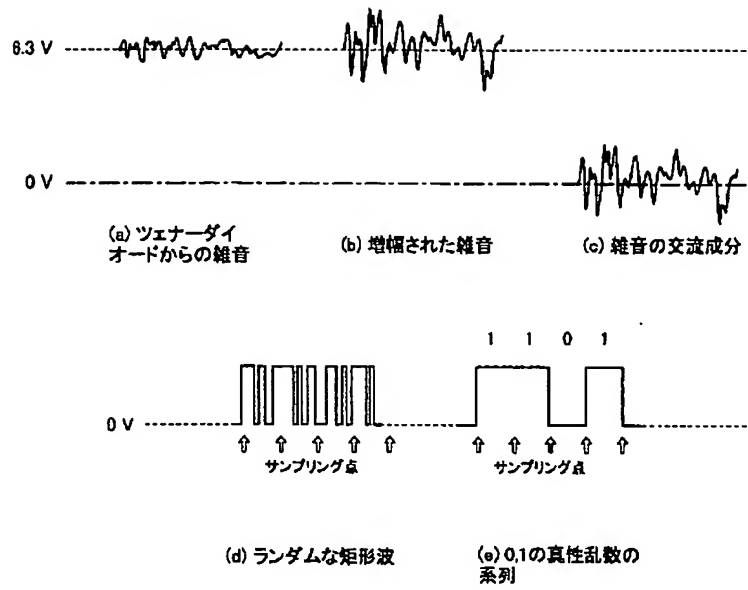
31 制御部

35 平滑部

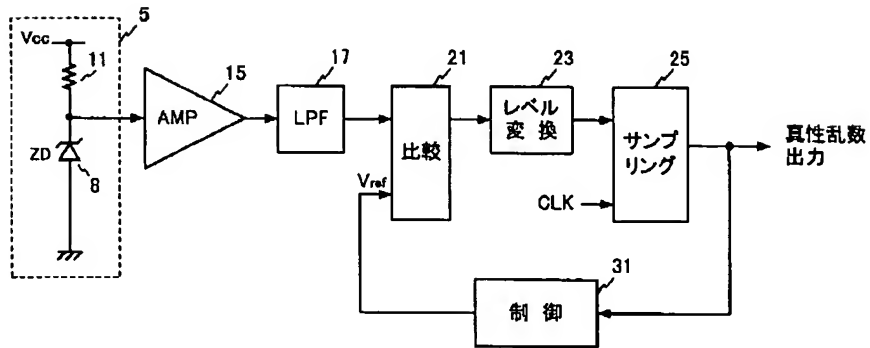
【図1】



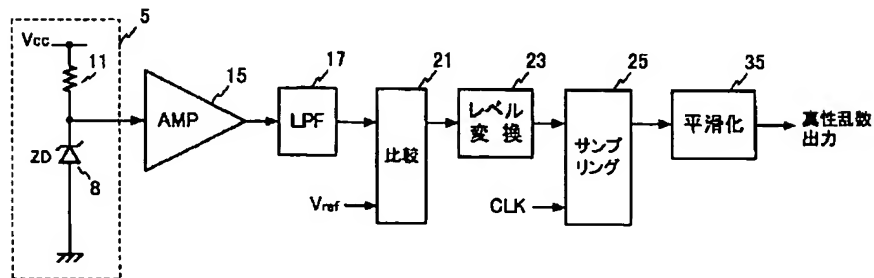
【図2】



【図3】



【図4】



【公報種別】特許法第 17 条の 2 の規定による補正の掲載
 【部門区分】第 6 部門第 2 区分
 【発行日】平成 13 年 7 月 19 日 (2001. 7. 19)

【公開番号】特開 2000-66592 (P2000-66592A)
 【公開日】平成 12 年 3 月 3 日 (2000. 3. 3)
 【年通号数】公開特許公報 12-666
 【出願番号】特願平 10-232823
 【国際特許分類第 7 版】

G09C 1/00 650

G06F 7/58

H03K 3/84

【F I】

G09C 1/00 650 B

G06F 7/58 A

H03K 3/84 Z

【手続補正書】

【提出日】平成 12 年 7 月 26 日 (2000. 7. 26)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項 1】 接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を前記接合に印加する逆バイアス印加手段と、前記接合を含む電流路に生ずる雑音信号の直流成分を除去する直流遮断手段と、当該直流成分除去信号をサンプリングして得られるサンプリング値系列を乱数として出力するサンプリング回路と、からなることを特徴とする乱数生成装置。

【請求項 2】 前記直流成分除去信号を所定の基準電圧

と比較して 2 値化信号を得る比較回路を更に有し、前記サンプリング回路は前記 2 値化信号をサンプリングすることを特徴とする請求項 1 記載の乱数生成装置。

【請求項 3】 前記半導体素子は、ツェナーダイオードであることを特徴とする請求項 1 又は 2 記載の乱数生成装置。

【請求項 4】 前記サンプリング値系列における 0 及び 1 の各々の発生確率が略等しくなるように前記基準電圧を制御する制御手段を有することを特徴とする請求項 2 又は 3 記載の乱数生成装置。

【請求項 5】 前記所定の基準電圧は接地電圧であることを特徴とする請求項 2 記載の乱数生成装置。

【請求項 6】 前記サンプリング値系列における 0 及び 1 の発生確率が略等しくなるように前記サンプリング値系列を平滑化する手段、を有することを特徴とする請求項 1 ないし 5 のいずれか 1 記載の乱数生成装置。